DATA SECURITY ACT OF 2006
SPONSORED BY SEN. BOB BENNETT AND SEN. TOM CARPER
SUMMARY
JUNE 23, 2006

COVERED ENTITIES

- Covers entities in the business of engaging in financial activities under section 4(k) of the Bank Holding Company Act and financial institutions.
- Also covers entities that maintain or possess information subject to the Fair Credit Reporting Act's disposal rule and any other entities that maintain or communicate sensitive personal or account information.
- Agencies are subject to separate safeguarding and notification duties.

COVERED INFORMATION

- Sensitive personal information – first and last name, address or telephone number, in combination with (1) SSN, (2) DLN, or (3) TIN. Excludes publicly available information.
- Sensitive account information – financial account number relating to a consumer, including a credit or debit card number, in combination with any security code, access code, password or other personal identification information required to access the financial account.
- Not limited to *customer* information.
- Includes paper as well as computerized data.

DATA SECURITY

- Covered entity must implement and maintain reasonable policies and procedures to protect the confidentiality and security of sensitive account and personal information maintained or communicated by or on behalf of such entity from unauthorized use that is reasonably likely to result in substantial harm or inconvenience to the consumer.
- Allows flexibility in customizing policies and procedures.

INVESTIGATION

- Following a security breach, covered entity must assess the nature and scope of the breach, identify any sensitive account or personal information involved in the breach, determine if such information is reasonably likely to be misused in a manner causing substantial harm or inconvenience to consumers.
- Covered entity to consider whether any neural network or security program has or will detect account fraud.

TRIGGER FOR NOTIFICATION

- Covered entities must notify if the information involved in a security breach is reasonably likely to be misused in a manner causing substantial harm or inconvenience to consumers.
- Exempts from definition of security breach information that is not usable to commit identity theft or account fraud, including information that is encrypted or redacted.

- Specifies that substantial harm or inconvenience does not include changing an account number or closing an account, nor harm or inconvenience resulting from something other than identity theft or account fraud (*e.g.* embarrassment).

BIFURCATED APPROACH TO NOTIFICATION

- Covered entity must notify (1) its functional regulator, (2) law enforcement, (3) the account-holding institution if the breach involves sensitive account information, (4) nationwide credit reporting agencies (CRAs) if the breach involves sensitive personal information and the number of affected individuals exceeds 5,000, and (5) affected consumers.

PREEMPTION

- Preempts state laws imposing obligations to: (1) protect the security of information relating to consumers; (2) safeguard information relating to consumers from potential misuse; (3) investigate or provide notice of unauthorized access to information relating to consumers or potential misuse of such information for fraudulent, illegal, or other purposes; or (4) mitigate any loss or harm resulting from unauthorized access or misuse of information relating to consumers.

SAFE HARBOR

- Financial institution deemed in compliance with safeguarding obligation if it maintains policies and procedures consistent with section 501(b) of GLB that cover non-customer as well as customer information.
- Financial institution deemed in compliance with investigation and notification obligations if it maintains policies and procedures consistent with section 501(b) of GLB that include investigation and notification to law enforcement, owners of financial accounts and CRAs as well as consumers.

ENFORCEMENT

- As in GLB, enforcement limited to functional regulators.
- Includes OFHEO as functional regulator for GSEs.
- Explicitly prohibits private rights of action.

RULEMAKING

- Functional regulators to prescribe content, method and timing of notice and allow delay for law enforcement reasons.
- Required consultation and coordination among functional regulators in issuing rules.

SERVICE PROVIDERS

- Regulations to require service providers to notify entity on whose behalf they are maintaining or communicate information following a security breach.
- Regulations also ensure that there is only one notification responsibility with respect to a security breach.